Office of Compliance and Ethics
UNIVERSITY of WEST FLORIDA

Procedure for Service Providers with Access to Cardholder Data

Area: Credit Cards
Purpose: Safeguard Cardholder Data for UWF Credit Card Customers
Reference: Payment Card Industry (PCI) Security Standards Council, Requirement 12.8

Procedures/ Requirements:

- These requirements apply to all outside service providers that have access to University of West Florida customer cardholder data:
- The University will perform the following procedures prior to establishing a formal relationship with a service provider:
    - Requests for Authorization (to accept credit card transactions) Forms submitted by departments will be reviewed by a delegate of the UWF PCI DSS Team from ITS, Financial Services or Compliance and Ethics. A determination will be made as to the services required, and whether those services will require the use of a service provider.
    - When it is determined that it is necessary to contract with a service provider, the contractors' proposals will be reviewed to evaluate the risks of loss of credit cardholder data. This evaluation will be a major factor in the award of such contracts.
- The University will maintain a list of service providers with access to cardholder data.
- Contracts with service providers must contain a written acknowledgment that "the service providers are responsible for security of cardholder data the service providers possess or otherwise store, process, or transmit on behalf of the University, or to the extent that they could impact the security of the University's cardholder data environment."
- Service providers are responsible for maintaining, and demonstrating compliance with, the Payment Card Industry Data Security Standards (PCI DSS).
- The University will verify each service provider's PCI DSS compliance at least annually, and before the award of any contract.

Questions/ Concerns:

Matt Packard, CCEP
Chief Compliance Officer
850.857.6070 | mpackard@uwf.edu

Reviewed September, 2026